**King Fahd University of Petroleum and Minerals**
**Information and Computer Science Department**

**ICS 254: Discrete Structures II**

**Programming Assignment**
**(Due Saturday April 28, 2018 at midnight)**

---

In this assignment, you will implement the *Diffie-Hellman* key agreement protocol. Before that, you will have to do the following:

1- (15 points) Explain the details of the *Diffie-Hellman* key agreement protocol. In doing so, you have to explain the following:
   a. The objective(s) of the protocol.
   b. How and under which restrictions/environment does it work?
   c. Determine which information can be made public and which information have to be made private.

2- (60 points) Implement the Diffie-Hellman key agreement protocol using Java, with the ability to use very large numbers. In this implementation, you should verify that the user input consisting of a prime number $p$ and a primitive root $a$ are valid. If not, the program should reject the current input and ask the user to enter correct input. The keys $k_1$ and $k_2$ are randomly generated.

**3- (70 points) BONUS: Try to break the security of this protocol by writing code that will generate the shared key as output.**

4- (15 points) Run your program with different values of $p$ and $a$ and show snapshots of the running of the program with different input values (invalid and valid).

5- (10 points) Include a small report that contains the following information:
   a. How to compile and run the code.
   b. Any specific details and/or algorithms that you have implemented, especially with regard to the BONUS part.
   c. The sample runs of your program that are described in Point "4".
   d. Who did what in the programming assignment.

Please note that you should do the implementation from scratch and without using any internet resources. Your answers will be verified by safeAssign and any copying of code among the groups or from the internet will result in a zero grade.

**IMPORTANT NOTES REGARDING YOUR SUBMISSION.**

Please submit your code and report as a single zip file.